Quelques rappels sur Netmagis

Emmanuel Halbwachs

Réunion DIO/ASR labos aka « Cisco », 11/10/2023

Observatoire de Paris, DIO

Rapidement pour les nouvelles personnes

Netmagis : quesako ?

- IPAM : *IP Address Management*
- Comme Efficient IP mais en logiciel libre
- `http://netmagis.org/`, développé par l'Université de Strasbourg
- Projet mort mais mûr, encore utilisable
- Fonctionnalités
  - référentiel adressage IP, FQDN et MAC
  - gestion des sous-réseaux déléguable à des ASR (vous)
  - génère automatiquement la configuration DNS et DHCP
- Données basiques associées à une adresse IP
  - type de machine
  - nom du responsable
  - informations complémentaires (champ libre)
- Mais Netmagis n'est pas un outil de gestion de parc (préférer GLPI)

Netmagis à l'Observatoire

- https://netmagis.obspm.fr/
- Extension maison DIO qui
  - augmente la base de données pour référentiel sous-réseau/VLAN
  - génère automatiquement la configuration Radius pour VLAN dynamiques par adresse MAC
- Vertu : cadre rigoureusement la gestion du DNS
- Documentation plutôt abondante
  - d'utilisation, pour vous les ASR
  - d'administration, de cas pratiques, pour la DIO
- Vous pouvez lire les fichiers de zones réels, copiés pour vous sur sionet

Rappels de gestion du TTL

Éviter les informations périmées en gérant le TTL en avance

TTL (*Time To Live*, durée de vie) : durée max. de conservation dans un cache de serveur DNS resolveur partout dans l'Internet.

Netmagis vous permer de gérer le TTL adresse par adresse, ◡̈
mais pas pour les alias. ◠̈

Lorsqu'il y a un changement dans la relation *hostname* ↔ adresse IP, c'est bien d'éviter les coupures de service en anticipant. Il faut alors gérer le TTL :

- le TTL par défaut est de 2 j
- au moins 2 j avant, passer le TTL à 1 h pour cette adresse
- au moins 1 h avant, passer le TTL à 5 min pour cette adresse
- faire le changement
- remettre le TTL par défaut pour cette adresse (supprimer le TTL spécifique)

Comment vérifier le TTL actuel d'un serveur externe ?

Il faut avoir accès à un serveur externe résolveur qui accepte la résolution récursive. C'est rare, ça peut être :

- celui de votre FAI lorsque vous y êtes connecté
- 8.8.8.8 (résolveur ouvert de Google)
- 9.9.9.9 (résolveur ouvert de CloudFlare)

Exemple 1/2 : résolveur de votre FAI

```
eh@bop:~$ dig www.obspm.fr

; <<>> DiG 9.19.17-1-Debian <<>> www.obspm.fr
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 26028
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.obspm.fr.                  IN      A

;; ANSWER SECTION:
www.obspm.fr.           7181    IN      CNAME   www2-prod.obspm.fr.
www2-prod.obspm.fr.     7181    IN      A       145.238.193.73
                        ^^^^
                          |------------------------------------------------ TTL (s)
;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)  <------------------------------ serveur
;; WHEN: Fri Oct 06 22:34:06 CEST 2023
;; MSG SIZE  rcvd: 81
```

Exemple 2 : résolveur ouvert de Cloudflare

```
eh@bop:~$ dig www.obspm.fr @9.9.9.9

; <<>> DiG 9.19.17-1-Debian <<>> www.obspm.fr @9.9.9.9
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33880
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;www.obspm.fr.                  IN      A

;; ANSWER SECTION:
www.obspm.fr.           43196   IN      CNAME   www2-prod.obspm.fr.
www2-prod.obspm.fr.     43196   IN      A       145.238.193.73
                        ^^^^^
                          |------------------------------------------------ TTL (s)
;; Query time: 8 msec
;; SERVER: 9.9.9.9#53(9.9.9.9) (UDP)  <---------------------------------- serveur
;; WHEN: Fri Oct 06 22:37:02 CEST 2023
;; MSG SIZE  rcvd: 81
```

Conseils

- si vous avez besoin de faire beaucoup de modifications (plusieurs dizaines)
- si vous avez besoin de modifier des alias (changement de cible d'un alias)

→ ticket DIO pour discuter de la modification du TTL de toute la zone (`obspm.fr`)

Résolution d'un nom de domaine seul, sans *hostname*

Adresse IP d'un nom de domaine seul sans *hostname*

Résolution par défaut pour un nom de domaine vers le site web (pratique) :

- `www.obspm.fr` → `145.238.193.73`
- `obspm.fr` → `145.238.193.73`
- il faut un enregistrement de type A sans nom
  - possible dans le préambule
  - non visible dans Netmagis par vous (uniquement DIO)
  - mais visible dans les fichiers de zones copiés sur sionet pour vous ☺

Domaines existants utilisables

```
obspm.fr

gepi.obspm.fr
imcce.obspm.fr
lerma.obspm.fr
lesia.obspm.fr
luth.obspm.fr
syrte.obspm.fr
ufe.obspm.fr

paas.obspm.fr
apps.paas.obspm.fr

padcpages.obspm.fr
pages.obspm.fr

ism.obspm.fr
```

Piège Netmagis : collision FQDN *vs* domaine

Un FQDN a deux parties, *host* et domaine. Exemple :

- www.obspm.fr
- www.lesia.obspm.fr

Que se passe-t-il si dans Netmagis on définit un *host* `lesia` dans le domaine `obspm.fr` ? Il y a coexistence dans la même configuration de deux objets différents qui donnent le même résultat :

- lesia.obspm.fr : host dans domaine
- lesia.obspm.fr : domaine tout court

→ le serveur DNS refuse de charger sa configuration et plus aucune requête ne résoud pour l'ensemble des zones (!)

→ bien avoir à l'esprit les noms de domaines existants

Quelques aspects de gestion et sécurité

De grands pouvoirs s'accompagnent de grandes responsabilités ◡̈

- tenir (raisonnablement) à jour les infos d'une machine
  - utile en cas d'incident SSI
  - si mise à jour en masse, ticket DIO pour discuter de la faisabilité
- éviter les données personnelles (nom, prénom) dans le *hostname*
  - le hostname est public
  - utiliser les infos associées plutôt que le *hostname*
- changer le hostname lorsqu'une machine change d'utilisateur
  - des droits peuvent être associée à un *hostname* (firewall)
  - ces droits ne doivent pas perdurer lorsque l'utilisateur change

Merci pour votre attention